REMARKS

Claims 1-41 are currently pending in the subject application, and are presently under consideration. Claims 1-41 are rejected. Claim 1 has been amended. Favorable reconsideration of the application is requested in view of the amendments and comments herein.

I. Rejection of Claims 1-41 Under 35 U.S.C. §103(a)

Claims 1-41 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Funk (US 5,721,779) in view of Keene, et al. (US PG Pub No. 2004/0049294). Withdrawal of this rejection is respectfully requested for at least the following reasons.

Claim 1, as amended, recites a method of administering access and security on a network having a plurality of computers. Messages broadcast or multicast within the network are filtered and displayed as-permitted by the associated privileges when a user's password is matched with the one-way encrypted password file. Claim 20 recites a system to administer access and security on a network having a plurality of computers. The system includes a channel monitoring and filtering module to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message. Finally, claim 31 recites a computer program for administering access and security on a network having a plurality of computers. The program includes a channel monitoring and filtering code segment to monitor and receive broadcast or multicast messages within the network and display the message to the user when the user's associated privileges permit the viewing of the message.

Neither Funk nor Keene teach the filtering and display of broadcast or multicast messages based upon user privileges, either alone or in combination. The Office Action notes that Funk does not teach this element, but cites a portion of the Keene patent as providing the required teaching. The Keene publication teaches a method for restricting access to data on a host computer. Each individual or organization that may have an interest in the data can access the host computer according to a password, with a given password granting access to certain

categories of data. The cited paragraph (7) merely describes this function. The Keene system does not include multicast or broadcast messages of data from the host computer. In fact, Keene teaches away from a multicast arrangement, providing a strongly hierarchical system in which all of the secured data is stored in a central database. Each of the guest computers query the host computer individually for desired data, with the access of the guest computers to the database controlled at a host computer. The host computer then responds to the querying computer with the desired data. A stated purpose of Keene is to provide a data sharing model where multiple users, representing competing companies, for example, can place information within the database without revealing the data to one or more other users. In fact, in one embodiment of the Keene device, the various users can be hidden from one another. It is respectfully submitted that Keene does not teach or suggest a teaching of a multicast or broadcast system.

A multicast message, by definition, must have at least two intended destinations. Accordingly, to monitor, receive, and selectively display multicast messages, a system would require structures at various points in the system to perform these functions. The Keene system does not contain the distributed filtering that would be required for the filtering of multicast messages as recited in claims 1, 20, and 31. The guest database privilege application (170) at each of the guest computers of Keene simply confirms the password of a given user and provides the confirmed user identity to the host computer along with a data request (*See* Keene, paragraph 40). The host computer determines if the guest computer possesses sufficient privilege to access the requested data and provides the requested data solely to requesting computer. All of the content and content filtering in Keene is centralized, making the Keene model unsuitable for a system incorporating multicasting. It is thus respectfully submitted that both Funk and Keene lack the required teaching of monitoring, receiving, and selectively displaying multicast messages, and that claims 1, 20, and 31 are allowable over the cited art.

Turning to the dependent claims, the applicant asserts that each dependent claim has its own specific limitations and features that define patentable invention over the prior art. For the sake of brevity, the discussion of certain dependent claims will be omitted. In focusing the

discussion on specific claims, a concession of the patentable distinctiveness of the others is not intended.

Claim 3 recites a method in which one or more attempts of the user entering a user identification and one-way encrypted password have failed to match the plurality of user identifications and one-way encrypted passwords contained in the one-way password encryption file. For such an occurrence, the method further includes transmitting notification to a systems administrator or security officer of the failure of the user to provide a user identification and one-way encrypted password that matches a user identification and one-way encrypted password stored on the one-way encrypted password file.

Funk does not discuss transmitting notification of failed log-in attempts to a system operator. The Office Action cites a passage within the Funk, discussing the challenge and response process used in authenticating a user. It does not suggest discuss the handling of a failed log-in attempt, beyond the obvious fact that access to the system would not be achieved. There is no suggestion of sending notification to a human operator of the failed log-in. Keene does not remedy this deficiency. Thus, it is respectfully submitted that claim 3 is nonobvious and patentable over the cited art both for its own elements and for those elements discussed in conjunction with claim 1.

Claims 5, 26, and 37 recite spoofing the user into believing that the access has been gained to the computer upon request of the systems administrator or security officer, wherein spoofing includes the presentation of false messages and information to the user.

Neither of the cited references discuss providing an unauthenticated user with false data in any form. The Office Action cites a portion of Funk describing the processing of the challenge signal at a processor associated with a central database, but there is no discussion of anything more than refusing to accept an incorrect password. The idea of providing false information to mislead an unauthenticated user is not suggested by this passage or any other portion of Funk. Keene also fails to teach or suggest spoofing a user accessing the system. Accordingly, it is respectfully submitted that claims 5, 26, and 37 are nonobvious and patentable over the cited art .

Claims 6, 25, and 36 recite disabling a computer system to prevent access by the user upon a request by the system administrator. Neither cited reference contains a teaching of disabling the system upon one or more rejections of user provided authentication. As discussed above, Funk and Keene simply provided for the rejection incorrect passwords and do not teach or suggest further action in response to multiple failed log-on attempts. The cited passage in Funk simply describes a randomization process for the encryption keys used in the authentication process. Accordingly, it is respectfully submitted that claims 6, 25, and 36 are nonobvious and patentable over the cited art.

Claim 7 recites deleting a plurality of files from the computer system upon a request by the systems administrator or security officer. Claims 25 and 36, discussed above, also include this element. Neither reference discusses remotely deleting system files to prevent an unauthorized user from accessing them. The Office Action cites a passage within the Funk, discussing the encrypted challenge and response process used in authenticating in a user. It is thus respectfully submitted that claims 7, 25, and 36 are nonobvious and patentable over the cited art.

Claims 8, 28, and 39 recite displaying a request for reauthentication at the direction of a system administrator or security officer. Claim 9, which depends from claim 8, requires that this reauthentication will take the form of a displayed log-in screen having a position for entry of the user identification and password. The Office Action cites two passages in Funk describing an initial authentication procedure. The claims, however, discuss reauthentication, requiring an already authenticated user to reenter a user identification and password just to maintain the present connection upon the request of a system administrator. Neither of the cited references discusses such a reauthentication process. It is thus respectfully submitted that claims 8, 28, 39, and 9 are nonobvious and patentable over the cited references.

Claim 11, which depends from claim 9, recites a method further including the following steps. A master password file is accessed on a computer system accessible to the system administrator or security officer. The password is one-way encrypted, and the master password file is searched for a match of the user identification and the one-way encrypted password.

Claim 13, which depends from claim 11, adds the following steps. An authenticated user enters a new password. The user identification and password stored on the master password file is reauthenticated. The new password is one-way encrypted, and the user identification and password in the master password file are replaced with the new user identification and the new one-way encrypted file.

Neither Funk nor Keene teach or suggest a password updating process initiated by a reauthentication request by the system administrator or security officer. The Office Action cites a passage within the Funk, discussing the encrypted challenge and response process used in authenticating in a user, but does not provide the required teaching. Accordingly, claims 11 and 13 are patentable over the cited art.

Claims 14, 29, and 40 recite attaching a master password file to a message, encrypting the message with a private key and passphrase available only to the systems administrator or security officer, and transmitting the message to the plurality of computers. Neither of the cited references contains such a teaching. The Office Action cites a passage in Funk discussing its challenge protocol in rejecting this claim. The cited passage does not address reauthorization or the updating of passwords on individual computers in the network. Keene does not remedy this deficiency. Accordingly, it is respectfully submitted that claims 14, 29, and 40 are thus nonobvious and patentable over the cited art.

Claims 15, 30, and 41 recite decrypting a message using a public key corresponding to the private key, reporting to the system administrator any failure to decrypt the message and replacing the one-way encrypted password file with the decrypted master file. The claims further recite notifying a system administrator if it receives a master password file that it cannot encrypt. This is intended to notify the system administrator of any attempts by an intruder to impersonate the system administrator. When the public key for the administrator fails to match the encryption key used for the file, it can be assumed that the file has been tampered with or otherwise falsified. Neither of the cited references teaches or suggests such a verification method. The passage cited in the Office Action discusses a method for updating passwords, but

does not teach notifying the system operator. It is thus respectfully submitted that claims 15, 30, and 41 are nonobvious and allowable over the cited art.

Dependent claims 2 – 19, 21-30 and 32-41 depend directly or indirectly from independent claims 1, 20, and 31, respectively. The applicant asserts that these claims are nonobvious and patentable for the reasons discussed above under their respective base claims and for their own unique elements.

For the reasons described above, claims 1-41 should be patentable over the cited art. Accordingly, withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing remarks, Applicant respectfully submits that the present application is in condition for allowance. Applicant respectfully requests reconsideration of this application and that the application be passed to issue.

Please charge any deficiency or credit any overpayment in the fees for this amendment to our Deposit Account No. 20-0090.

Respectfully submitted,

Date 7/08/07

Christopher P. Harris
Registration No. 43,660

CUSTOMER NO.: 26,294

TAROLLI, SUNDHEIM, COVELL, & TUMMINO L.L.P.
526 SUPERIOR AVENUE, SUITE 1111
CLEVELAND, OHIO 44114-1400
Phone: (216) 621-2234
Fax: (216) 621-4072